REMARKS

In the final Office Action, the Examiner objected to Claim 25 under 37 C.F.R. 1.75(c) as being in improper form. In response, applicants respectfully note that although Claim 25 is a multiple dependent claim, it does *not* depend from any other multiple dependent claim. Therefore, Claim 25 is in proper form.

Claims 1-6, 8-21, and 23-26, were finally rejected under 35 U.S.C. § 103(a) as being unpatentable over Shen (U.S. Patent No. 6,611,850) in view of Falkner (U.S. Patent No. 5,713,008). Applicants respectfully traverse the rejection of these claims.

Prior to discussing why these claims are allowable over the cited and applied references, a brief description of an embodiment of the claimed invention is set forth below. It is noted that the following is provided merely to assist the Examiner's understanding of the present invention and is not intended to limit the scope of the claims.

In one aspect, the invention is directed to computer intruder detection. For example, a server computer may be associated with a log file that records computer system operations of the server, such as deletion of a file. Thus, even if an intruder could delete a file on the server, so long as its associated log file is protected from unauthorized alteration or deletion, an administrator of the server could determine (based on the log file) that the file has been deleted and take a remedial action (e.g., restoring the file using a back-up file). If, however, the log file itself is altered or deleted to thereby erase the trace of an intruder action, then the server administrator will not even know whether or what type of unauthorized action has taken place. It is therefore imperative to maintain the integrity of a log file, and the present invention is directed to achieving this goal.

LAW OFFICES OF
CHRISTENSEN O'CONNOR JOHNSON KINDNESS PLLC
1420 Fifth Avenue
Suite 2800
Seattle, Washington 98101
206.682.8100

In one embodiment, a log file protection system of the invention comprises "log file creation means," "alteration detection means," and "restoration means." The log file creation means creates "*a plurality of identical log files* which record the operations of [a] computer system." The alteration detection means then "*periodically monitors*" the "*plurality of identical log files*" for alteration or deletion. When the alteration detection means detects an altered or deleted log file (among the plurality of identical log files), the restoration means restores the altered or deleted log file by replacing it with an unaltered log file from the "*plurality of identical log files*." Thus, according to an embodiment of the present invention, a plurality of identical log files are created and periodically monitored so that even if one of the identical log files should be altered or deleted, an altered or deleted log file can be replaced with another of the identical log files that has not been altered or deleted. The invention is based on the reality that an intruder, even if he/she could alter or delete one log file, is unlikely to be able to alter or delete all the identical log files at the same time. (An intruder will not even know whether or how many of a plurality of identical log files are stored.) Therefore, as long as at least one of the identical log files remains unaltered and undeleted, this unaltered and undeleted log file can be used to replace any log file that has been altered or deleted, to thereby maintain the integrity of the identical log files as a whole.

Claims 1 and 26 explicitly recite the creation and periodic monitoring of the "plurality of identical log files" as discussed above. Applicants respectfully point out that Shen and Falkner, either alone or in combination, do not disclose or suggest the claimed feature directed to the creation and periodic monitoring of the "plurality of identical log files."

Specifically, Shen is not even related to a "log file" protection system, but rather is related to a conventional file backup/restore method. Furthermore, though Shen teaches creating

LAW OFFICES OF
CHRISTENSEN O'CONNOR JOHNSON KINDNESS PLLC
1420 Fifth Avenue
Suite 2800
Seattle, Washington 98101
206.682.8100

a plurality of backup files for each file, these backup files are created at different times and therefore are *not* identical to each other. Specifically, Shen describes:

> [T]he backup/restore control apparatus...includes...a "backup generation control means"...*to generate a backup copy at pre-set timing every time the designated file(s)* selected during the above-mentioned "backup file selecting means" *is/are created or updated.*
>
> (Col. 5, lines 9-17, emphasis added.)

Shen teaches creating backup files at different times ("every time the designated file is created or updated") so that if any file is corrupted with a virus then the corrupted file can be replaced with a backup file that was stored prior to the time of corruption. To that end, Shen employs a "generation management unit 215 to manage the past status of these file(s)." (Col. 12, lines 28-32). More specifically, Shen describes:

> [T]he third objective [of the invention] is, to enable easy restoration of the original file(s) *to a state of designated time period backing from the current time*, using the backed-up file(s).
>
> Then, the fourth objective is, while this invention makes possible to easily restore the files to a state of designated time period backing from the current time, to enable *the management of past state of these files using the backed-up copy[ies].*
>
> (Col. 2, lines 58-65, emphasis added.)
>
> By this method of taking a backup for all the modified file has the following advantage. That is, even if a file was infected by a virus that cannot be detected by a virus checker, *it is possible to restore back to a version of that file before getting infected.* But then, *since there may be many versions (generations) of the backed-up files*, it is very difficult to find a particular version, so in this form of implementation, a pre-defined "time period" is set at backup information setting unit 211, and restore the designated file.
>
> (Col. 16, lines 39-47, emphasis added.)

In short, in Shen, a backup file is created "every time the designated file is created or updated," and therefore "many versions (generations) of the backed-up files" may be created over time, which obviously are *not* identical to each other.

Accordingly, Shen does not teach or suggest creating and periodically monitoring "a plurality of identical log files" as recited in Claims 1 and 26. To the contrary, Shen explicitly teaches creating "many versions (generations)" of backup files, which actually teaches *away* from creating "a plurality of identical log files" as recited in Claims 1 and 26. Furthermore, Shen does not at all teach or suggest "periodically monitor[ing] said plurality of identical log files for alteration or deletion" as recited in Claims 1 and 26. Rather, in Shen:

> [A]n "integrity judgment process" will judge the integrity of the designated file when making a backup copy of such file during the "backup copy generation process," and only if the result of above-mentioned "integrity judgment process" prove to be positive (i.e., not infected by a virus of destroyed,) then it will generate a backup copy of the designated file.
>
> (Col. 3, line 66-Col. 4, line 6.)

In other words, Shen monitors only the "designated file" (i.e., the original file) to see if it is "infected by a virus or destroyed," and if not creates its backup copy. Shen is not at all monitoring any *backup copy* to see if it has been infected or destroyed, and as such, Shen does not teach or suggest "periodically monitor[ing] *said plurality of identical log files* for alteration or deletion" (emphasis added) as recited in Claims 1 and 26.

Based on the foregoing reasons, it is respectfully submitted that Claims 1 and 26 are allowable over Shen.

With respect to Falkner, applicants merely note that Falkner does not disclose or suggest the creation or periodic monitoring of "a plurality of identical log files," and therefore cannot cure the deficiency of Shen. Accordingly, Claims 1 and 26 are allowable over Shen and Falkner even in combination.

Claims 2-6, 8-21, and 23-25 are all dependent from Claim 1, and therefore are allowable for at least the same reasons why Claim 1 is allowable.

LAW OFFICES OF
CHRISTENSEN O'CONNOR JOHNSON KINDNESS PLLC
1420 Fifth Avenue
Suite 2800
Seattle, Washington 98101
206.682.8100

In closing, based on the above, applicants respectfully request the Examiner to reconsider his previous finding and allow Claims 1-6, 8-21, and 23-26 of the present application.

Respectfully submitted,

CHRISTENSEN O'CONNOR
JOHNSON KINDNESS[PLLC]

Shoko I. Leek
Registration No. 43,746
Direct Dial No. 206.695.1780

I hereby certify that this correspondence is being deposited with the U.S. Postal Service in a sealed envelope as first class mail with postage thereon fully prepaid and addressed to Mail Stop AF, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450, on the below date.

Date: 6/8/05

SIL:jam

LAW OFFICES OF
CHRISTENSEN O'CONNOR JOHNSON KINDNESS[PLLC]
1420 Fifth Avenue
Suite 2800
Seattle, Washington 98101
206.682.8100